Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: Tuesday 9am	**Entry:** 1
Description	A small U.S. healthcare clinic experienced a ransomware attack. An employee opened a phishing email containing a malicious attachment. Once the attachment was downloaded, it installed malware that encrypted critical organizational data. A ransom note was displayed, demanding payment in exchange for a decryption key.
Tool(s) used	Not specified in the scenario, but common tools for response may include: antivirus software, network monitoring tools, endpoint detection and response (EDR), and backup recovery tools.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of unethical hackers. ● **What** happened? The employee downloaded a malicious attachment from a phishing email, which led to ransomware being deployed. ● **When** did the incident occur? Tuesday at approximately 9:00 a.m.

	● **Where** did the incident happen? At a small U.S. healthcare clinic specializing in delivering primary care services. ● **Why** did the incident happen? An employee opened a phishing email without recognizing it as suspicious, allowing malware to install and encrypt files.
Additional notes	Include any additional thoughts, questions, or findings. Why weren’t employees trained to detect and avoid phishing attempts? Was antivirus or email filtering in place to block malicious attachments? This incident highlights the need for user awareness training, endpoint protection, and a solid incident response plan.